ČSOB BUSINESS CONNECTOR

IMPLEMENTATION GUIDE TO DOWNLOADING AND UPLOADING FILES AUTOMATICALLY

Notice of changes from 20 October 2024

- New version of GetDownloadFileList v4 – older versions are still applicable only for contracts, where there are no uploads.
- New version of StartUploadFileList v3 – change hash algorithm from MD5 to SHA256, do not use old versions anymore.
- New version of FinishUploadFileList v2 – change hash algorithm from MD5 to SHA256, do not use old versions anymore.
- Only Multipart is usable for file upload, do not use octet-stream anymore.
- A transition period will be available for these changes until 31 March 2025 when the services will be concurrently usable. After this date, original Services will be switched off.

If you have any questions, please contact Helpdesk CEB.

CONTENT

1 INTRODUCTION

This guide contains user and technical documentation relating to the implementation of the ČSOB Business Connector service for ČSOB CEB, which will allow the customer to automatically communicate with the bank by transferring files, such as account statements, advices and exchange rates from the bank to the client, and batch payment orders from the client to the bank.

The guide also includes a technical description of the interface the bank provides for the implementation of a client application in the client's environment or for the integration of this interface into third-party software.

The bank also provides a basic client application for automated communication for Windows and Linux. It is available for download.

2 GETTING STARTED WITH THE ČSOB BUSINESS CONNECTOR SERVICE

In order to successfully connect to the ČSOB Business Connector service, several conditions must be met, and the application installed on a client computer must be connected to the service at the bank. To do this, the service uses electronic certificates, which guarantee the identity of the client and protect the transmission channel.

Take the following steps to be able to use the service:

- **enable the** ČSOB Business Connector **service** in the Agreement on the Use of ČSOB CEB Service;
- **obtain a certificate** from a certification authority or directly from the bank;
- **register the certificate** for use in the ČSOB Business Connector service on the CEB portal;
- **configure the** ČSOB Business Connector **service** on the CEB portal;
- **implement** your own **client application**;
- or download, install and configure the **basic client application** provided by the bank.

2.1 Enabling the ČSOB Business Connector service in the Agreement on the Use of ČSOB CEB Service

As specified in the CEB service business terms and conditions, the ČSOB Business Connector service is enabled by default for all clients unless requested otherwise.

The ČSOB Business Connector service can be disabled or enabled via the CEB portal.

2.2 Obtaining a certificate

Certificates suitable for use in the ČSOB Business Connector service can be obtained from so-called certification authorities. These companies issue an electronic certificate to the customer based on the information provided and after checking that the information is valid. The issued certificate has a limited validity (usually 1 year) and must be renewed before it expires. I.e. a new (follow-up) certificate with a new validity must be issued.

The ČSOB Business Connector service allows you to use certificates issued by the certification authorities První certifikační autorita and PostSignum.

Certification authorities (CAs) issue a variety of certificates of various types and for various purposes. Only so-called commercial server certificates, which support the so-called client authentication, are suitable for use in the ČSOB Business Connector service. If in doubt, contact your certification authority directly.

The online process of obtaining a certificate includes:

- creating a private key and an electronic certificate request on a client computer;
- sending the electronic request to a CA, processing the request in the CA and issuing the certificate;
- downloading the issued certificate and installing it on the client computer.

The certificate can also be obtained directly from the bank by clicking on **Request certificate** on the Business Connector settings page on the CEB portal. See the following chapter.

2.2.1 Obtaining a certificate from the bank

This procedure must be done on a computer that is running the ČSOB Business Connector client application. A private key will be created, which will be merged with the issued certificate at the end and which will be available to the application.

2.2.1.1 Creating a certificate request manually on a client computer

The first step to obtaining a certificate is to create an electronic certificate request. Depending on the platform on which the Business Connector client application is running, select:

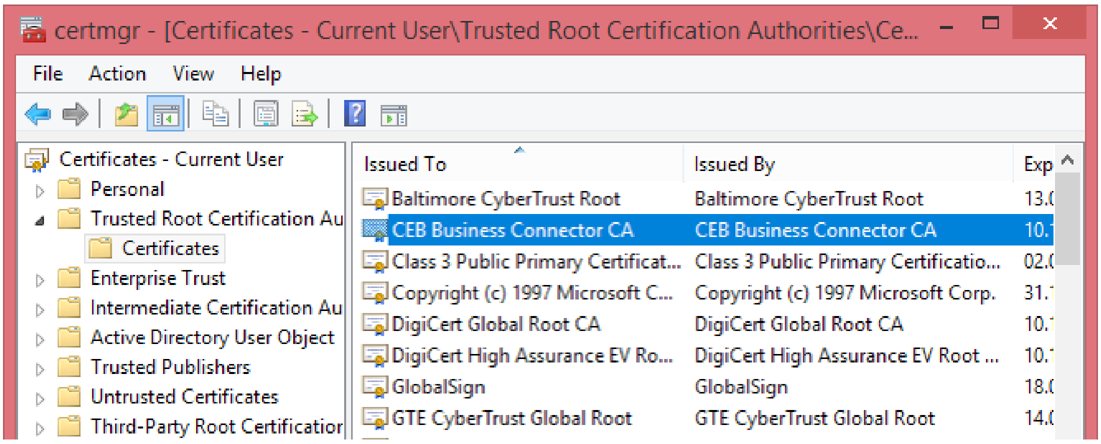
- the **certreq.exe** Windows tool,
  if the application is running on Windows and you want to save the certificate to a certificate store of the operating system;
- **openssl**,
  if the application is running on Linuxu, MacOS or Windows and you want to save the certificate as files;
- Java **keytool**,
  if the application is running as a Java application on Linuxu, MacOS or Windows.

2.2.1.1.1 Using certreq.exe (part of Windows)

Before you start the process, a root certificate of the issuer (the bank) must be installed on your computer. This certificate must be placed among the trusted root certification authorities.

Press **Windows + R**, type certmgr.msc in the box and press OK.

In the certmgr tool, expand *Trusted root certification authorities, Certificates* on the left and look up the CEB Business Connector CA line on the list.



certmgr - [Certificates - Current User\Trusted Root Certification Authorities\Ce...

- Certificates - Current User
  - Personal
  - Trusted Root Certification Au
    - Certificates
  - Enterprise Trust
  - Intermediate Certification Au
  - Active Directory User Object
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certificatior

Issued To	Issued By	Exp
Baltimore CyberTrust Root	Baltimore CyberTrust Root	13.0
CEB Business Connector CA	CEB Business Connector CA	10.1
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	02.0
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	31.1
DigiCert Global Root CA	DigiCert Global Root CA	10.1
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	10.1
GlobalSign	GlobalSign	18.0
GTE CyberTrust Global Root	GTE CyberTrust Global Root	14.0

If the line is missing, download the issuer's certificate from https://www.csob.cz/portal/documents/10710/15532355/cebbc-ca.crt. In the certmgr tool, right click on **Certificates** in the **Trusted root certification authorities** folder, select All Tasks – Import..., and then select the issuer's certificate you've downloaded.

In order to manually create a certificate request using a command line and tool certreq.exe, you must first create a text file that contains a request template specified below. To do this, use Notepad (notepad.exe; do not use Word). Please note that some editors insert an invisible mark, a so-called BOM, at the beginning of files. Save your file as ASCII or UTF-8 without BOM.

```
[NewRequest]
Subject="CN=<BC server>, C=CZ"
KeySpec=1
HashAlgorithm=sha256
KeyLength=2048
UseExistingKeySet=FALSE
Exportable=TRUE
UserProtected=FALSE
MachineKeySet=FALSE
ProviderName="Microsoft RSA SChannel Cryptographic Provider"
ProviderType=12
RequestType=PKCS10
KeyUsage=0xa0
SMIME=False
SuppressDefaults=true
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.2
```

In the template, specify the computer name on the Subject= line; enter the name behind the CN= characters. The name must not contain a comma (,) or a quotation mark ("). The name will be included in the name of the issued certificate.

Save the template file; name it e.g. BCcert.inf and save it to Documents.

Press **Windows + R** and type cmd.exe in the box and press OK.

A command line will open; type the cd and certreq commands:

```
C:\Users\Novák> cd Documents
C:\Users\Novák\Documents> certreq -new BCcert.inf BCcertreq.req
CertReq: Request Created
```

The request you've created will be saved to the BCcertreq.txt file, which can be viewed and copied as text (the file consists of base64-encoded binary data):

```
C:\Users\Novák\Documents> notepad.exe BCcertreq.req
```

Your certificate request file must be transferred to the computer you're using for logging in to CEB.

The private key that has been created as described above has been saved to the Windows certificate store and will be merged with the issued certificate in the last step. It is therefore necessary to complete this process on the same computer on which it started.

2.2.1.1.2 Using openssl (all platforms)

In order to create a certificate request using openssl, first create a request configuration text file according to the example below:

```
[ req ]
default_bits = 2048
default_md = sha256

distinguished_name = req_distinguished_name
prompt = no
string_mask = nombstr
encrypt_key = no

[ req_distinguished_name ]
C = CZ
CN = <BC server>
```

On the "CN =" line, enter the name of the computer you will use to connect to the Business Connector service. This name will then be included in the name of the issued certificate. Save the configuration file e.g. to the current directory and name it (e.g. bccert.cnf).

Then run the following command in this directory:

```
[user@mycomp ~]$ openssl req -config bccert.cnf -new -keyout bccert.key -out bccert.csr
```

The private key has been saved to the bccert.key file. Keep this file on the computer. You will need the file as well as the certificate you'll get in the next step to establish a connection with the CEB BC service. It is advisable to restrict read access rights of the file using the following command:

```
[user@mycomp ~]$ chmod 400 bccert.key
```

The request will be saved as the bccert.csr file, which can be viewed and copied as text (the file consists of base64-encoded binary data). Transfer this file to the computer you are using to log in to CEB.

2.2.1.1.3 Using Java keytool (all platforms)

In order to create a JKS file and a then certificate request using the Java keytool, run the following commands (you will be prompted to enter a new password):

```
[user@mycomp ~]$ keytool -genkey -alias bccert -keyalg RSA -keysize 2048 -dname "CN=<BC server>,C=CZ"
-keystore bccert.jks
```

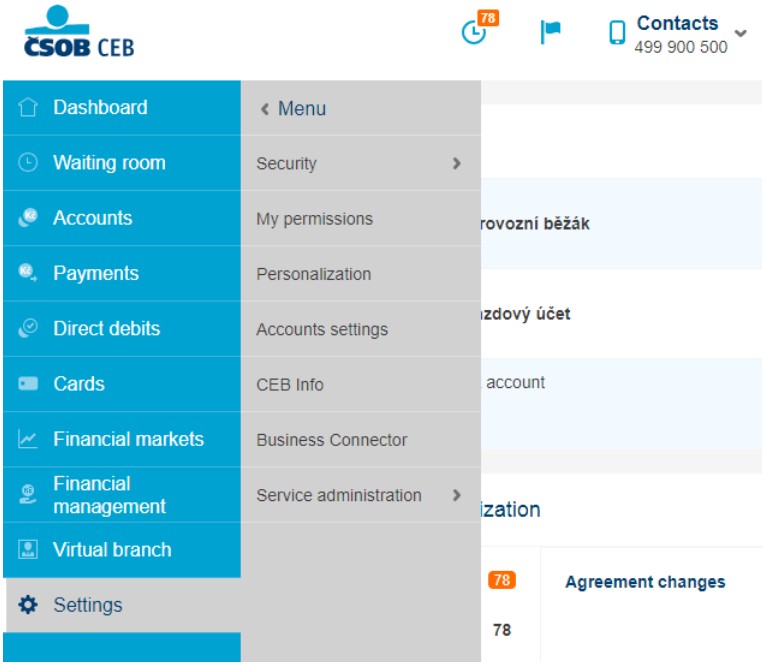
Enter the name of the computer you will use to connect to the Business Connector service instead of <BC server>. This name will then be included in the name of the issued certificate.

```
[user@mycomp ~]$ keytool -certreq -alias bccert -keyalg RSA -file bccert.csr -keystore bccert.jks
```

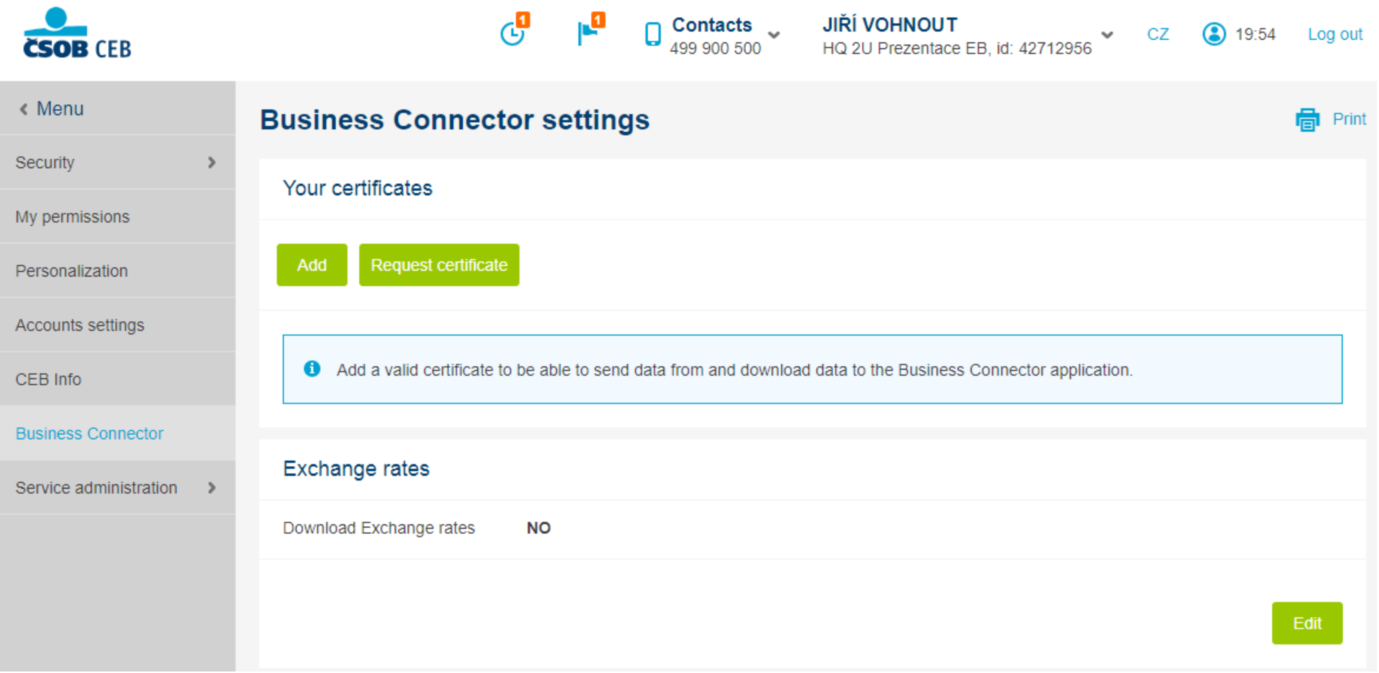
The private key has been saved to the bccert.jks JKS file and is waiting for the import of the issued certificate. The request will be saved as the bccert.csr file. Transfer this file to the computer you are using to log in to CEB.

2.2.1.2 Submitting the certificate request and getting a certificate

After logging in to CEB, open the menu, go to Settings > Business Connector.



Press the *Request certificate* button,



Business Connector settings

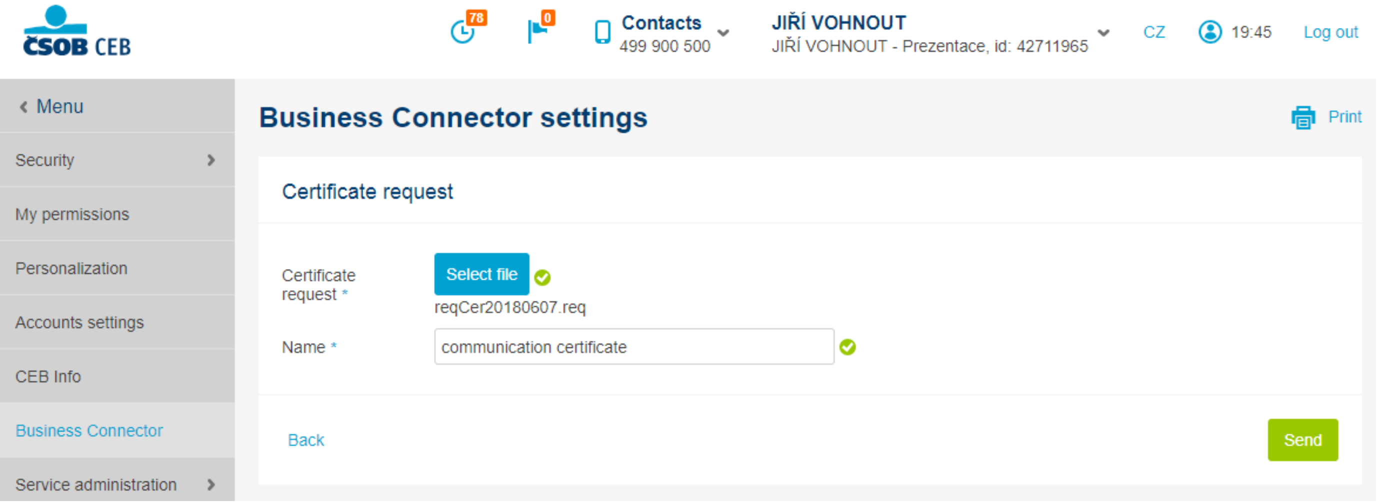
Your certificates

Add a valid certificate to be able to send data from and download data to the Business Connector application.

Exchange rates

Download Exchange rates NO

fill in the *Certificate name* and *select the certificate request file* (see 2.2.1.1 Creating a certificate request manually on a Windows client computer), then press the *Send* button to confirm.



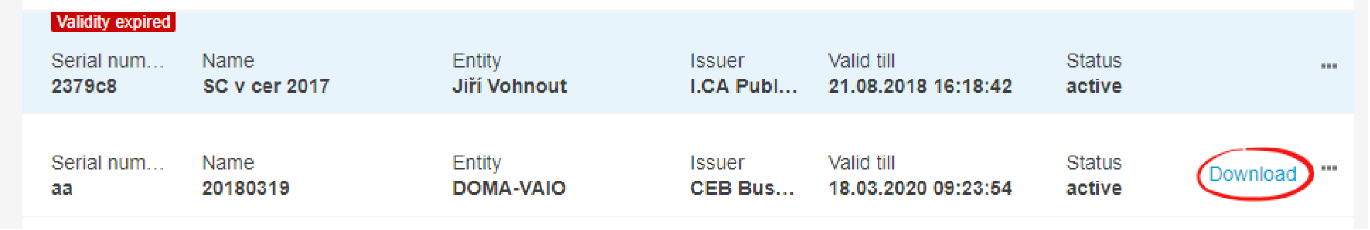
Business Connector settings

Certificate request

Certificate request * reqCer20180607.req

Name * communication certificate

Download the issued certificate.



Serial num...	Name	Entity	Issuer	Valid till	Status
2379c8	SC v cer 2017	Jiří Vohnout	I.CA Publ...	21.08.2018 16:18:42	active
aa	20180319	DOMA-VAIO	CEB Bus...	18.03.2020 09:23:54	active

2.2.1.3 Installing the issued certificated on a client computer

The final step is to install the issued certificate on the client computer, as described in step 1. Follow the procedure suitable for the selected option; see chapter 2.2.1.1.

2.2.1.3.1 Using certreq.exe (part of Windows)

Install the file BCcert.cer that contains the issued certificate on the computer you used to create the certificate request:

```
C:\Users\Novák> cd Documents
C:\Users\Novák\Documents> certreq –accept BCcert.cer
```

2.2.1.3.2 Using openssl (all platforms)

Transfer the bccert.crt certificate file back to the computer on which you created the certificate request.

Now you have the bccert.key (private key) and bccert.crt (certificate) files, which, depending on implementation, can be either used separately by the client application or merged into one PKCS12 file using the following command:

```
[user@mycomp ~]$ openssl pkcs12 -export -in bccert.crt -inkey bccert.key -out bccert.p12
```

2.2.1.3.3 Using Java keytool (all platforms)

Install the bccert.cer certificate file on the computer on which you created the certificate request into the JKS file created in step 1. You must first import the issuing authority's certificate cacert.cer using the command below. You will be asked if you trust this certificate; answer yes.

```
[user@javacomp ~]$ keytool –importcert -alias cacert -file cacert.cer -keystore bccert.jks
```

And then import the issued certificate to the same JKS file using the following command:

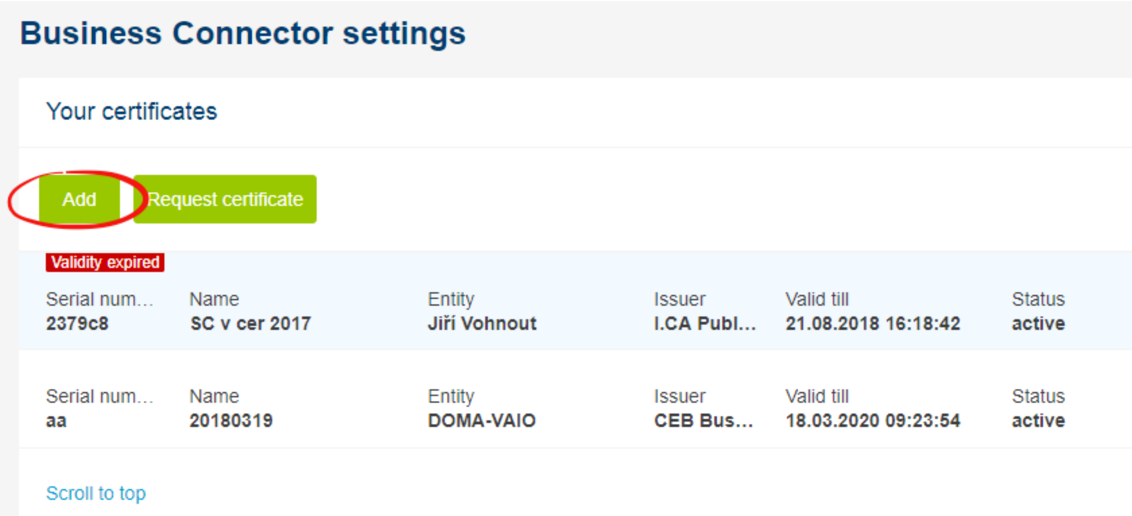
```
[user@mycomp ~]$ keytool -import -alias bccert -file bccert.cer
-keystore bccert.jks
```

2.3 Registering a certificate in the CEB service

The list of the certificates that authorize users to download and upload files via the ČSOB Business Connector can be managed on the CEB portal.

If your certificate has been issued by the bank, you can click on the Request certificate button to add the certificate directly to the list of registered certificates. It is not necessary to register the certificate file by clicking on the *Add certificate* button.

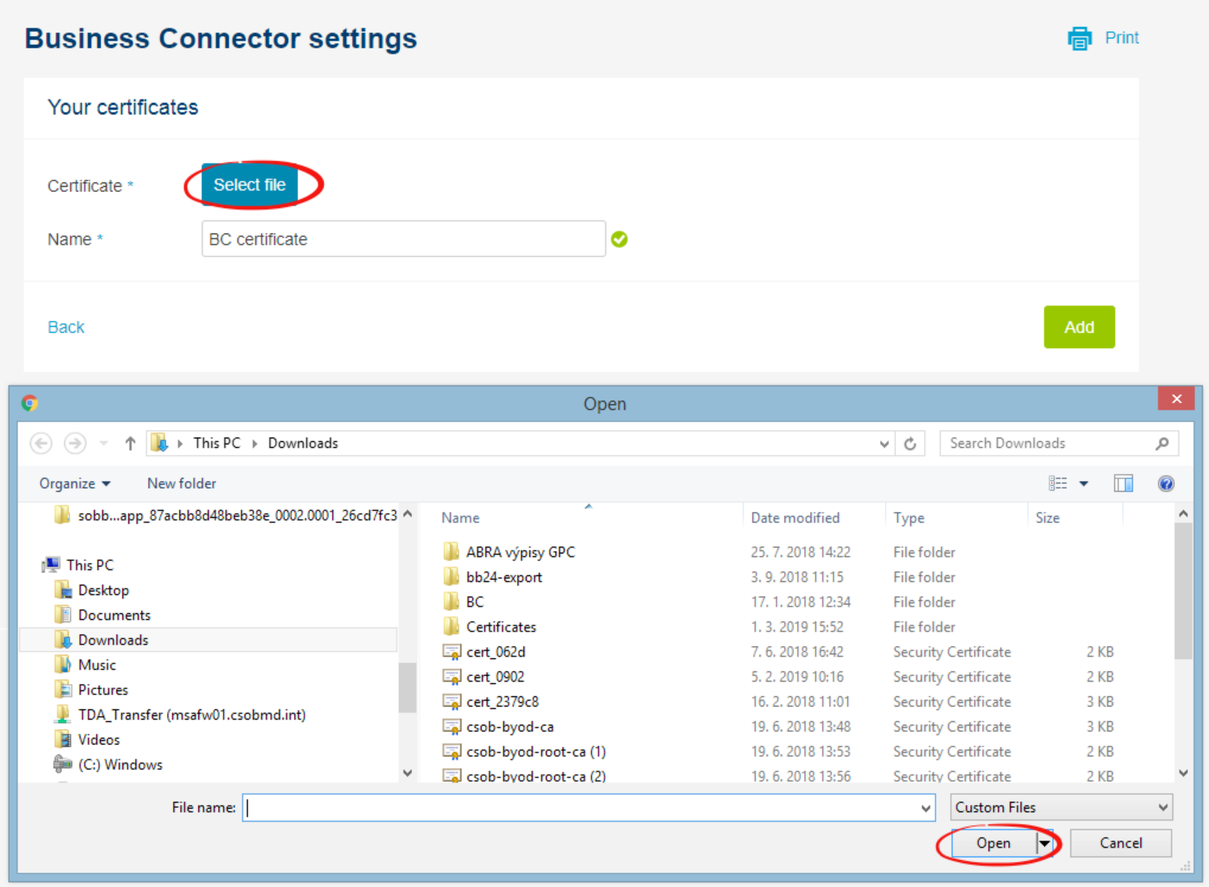
A certificate issued by a certification authority except for the bank must be added to the list by clicking on the *Add certificate* button in order to register the certificate.



Validity expired

Serial num...	Name	Entity	Issuer	Valid till	Status
2379c8	SC v cer 2017	Jiří Vohnout	I.CA Publ...	21.08.2018 16:18:42	active
aa	20180319	DOMA-VAIO	CEB Bus...	18.03.2020 09:23:54	active

If you obtained your certificate in a different way, it is necessary to add it to the list of registered certificates belonging to the agreement by clicking on the *Add certificate* button.



Certificate *

Name * BC certificate

Name	Date modified	Type	Size
ABRA výpisy GPC	25. 7. 2018 14:22	File folder	
bb24-export	3. 9. 2018 11:15	File folder	
BC	17. 1. 2018 12:34	File folder	
Certificates	1. 3. 2019 15:52	File folder	
cert_062d	7. 6. 2018 16:42	Security Certificate	2 KB
cert_0902	5. 2. 2019 10:16	Security Certificate	2 KB
cert_2379c8	16. 2. 2018 11:01	Security Certificate	3 KB
csob-byod-ca	19. 6. 2018 13:48	Security Certificate	3 KB
csob-byod-root-ca (1)	19. 6. 2018 13:53	Security Certificate	2 KB
csob-byod-root-ca (2)	19. 6. 2018 13:56	Security Certificate	2 KB

File name:

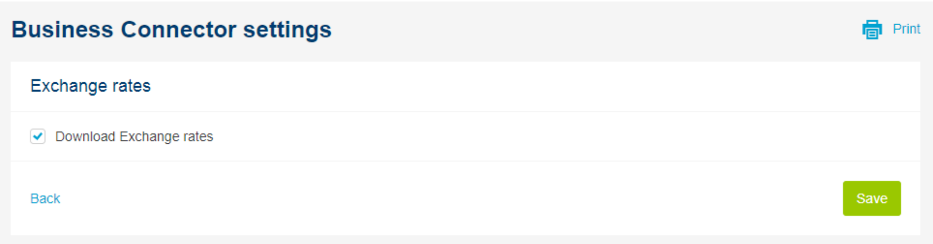
Open the certificate file by clicking on *Select file*, fill in the *Certificate name*, and then press the *Import* button to register the certificate to the selected agreement.

2.4 Configuring the service on the CEB portal

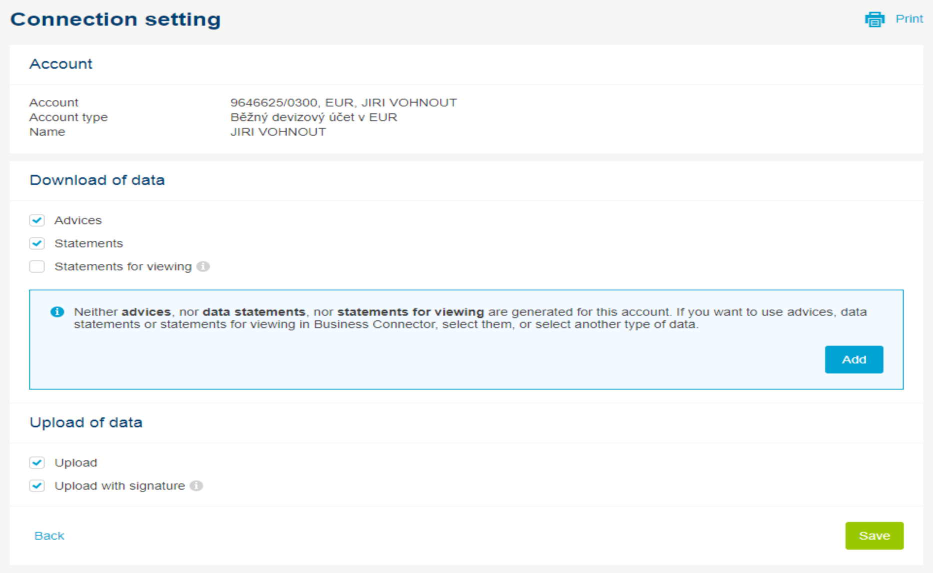
The features the client will be allowed to use via the ČSOB Business Connector need to be enabled on the CEB portal.

You can enable:

- downloading exchange rates (CNB and ČSOB);
- downloading statements for selected accounts;
- downloading advices for selected accounts;
- sending payment order files for selected accounts;
- sending signed payment order files for selected accounts.



☑ Download Exchange rates



Connection setting

Account

Account	9646625/0300, EUR, JIRI VOHNOUT
Account type	Běžný devizový účet v EUR
Name	JIRI VOHNOUT

Download of data

☑ Advices

☑ Statements

□ Statements for viewing

Neither **advices**, nor **data statements**, nor **statements for viewing** are generated for this account. If you want to use advices, data statements or statements for viewing in Business Connector, select them, or select another type of data.

Upload of data

☑ Upload

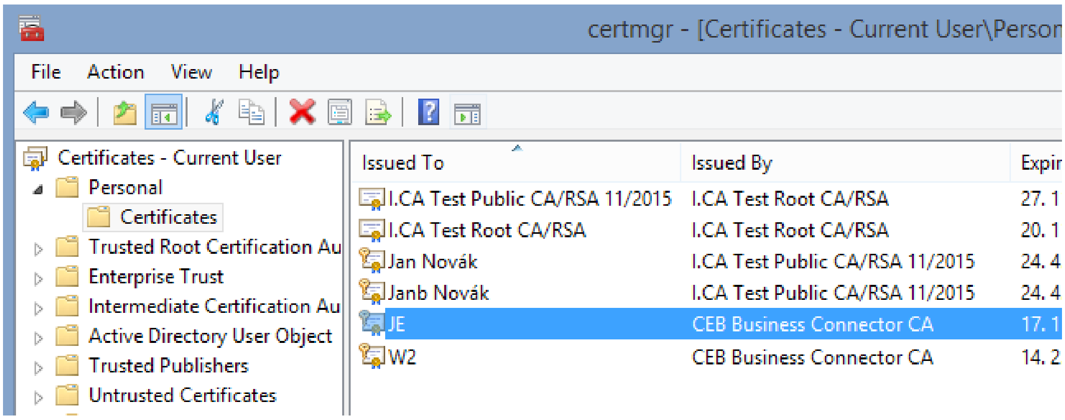
☑ Upload with signature

2.5 Backing up a certificate and a private key

We recommend that you back up both your certificate and private key according to the following procedure. Backing up the certificate file (*.cer or *.crt) only is not sufficient e.g after a hardware error or after reinstalling the operating system because this file does not contain a private key.

Press **Windows + R**, type certmgr.msc in the box and press OK.

In the certmgr tool, expand *Personal* on the left and look up your certificate. Its issuer will be CEB Business Connector CA and it will bear the name you've chosen.



certmgr - [Certificates - Current User\Persor

File
Action
View
Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates

Issued To	Issued By	Expir
I.CA Test Public CA/RSA 11/2015	I.CA Test Root CA/RSA	27. 1
I.CA Test Root CA/RSA	I.CA Test Root CA/RSA	20. 1
Jan Novák	I.CA Test Public CA/RSA 11/2015	24. 4
Janb Novák	I.CA Test Public CA/RSA 11/2015	24. 4
JE	CEB Business Connector CA	17. 1
W2	CEB Business Connector CA	14. 2

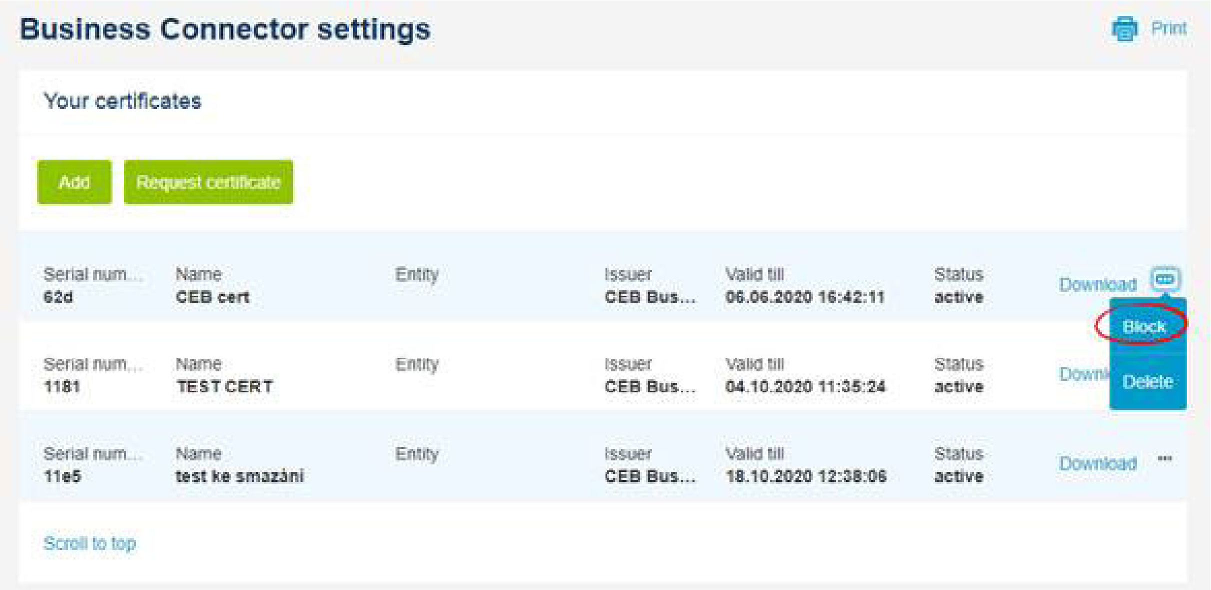
Right click on the certificate and select *All tasks > Export...* from the context menu.

In the certificate export wizard, select *Yes, export private key*, and then export the private key to the PKCS #12 file with the .pfx extension.

2.6 Revoking a certificate due to the compromised key

In the event of a loss or misuse of your certificate's private key (stolen computer, hacker attack, unauthorized use by an employee, etc.), you are obliged to revoke the certificate. In such a case, follow the standard procedure of your certification authority (I. CA, PostSignum). The certificate will be blocked, and it won't even communicate with the ČSOB Business Connector service in the bank.

It is also advisable to block or completely remove the certificate in the ČSOB Business Connector administration on the CEB portal, where you registered the certificate.



Serial num...	Name	Entity	Issuer	Valid till	Status
62d	CEB cert		CEB Bus...	06.06.2020 16:42:11	active
1181	TEST CERT		CEB Bus...	04.10.2020 11:35:24	active
11e5	test ke smazáni		CEB Bus...	18.10.2020 12:38:06	active

No revocation procedure has been defined for certificates issued by the bank.

Use the ČSOB Business Connector administration interface on the CEB portal to block a compromised certificate issued by the bank. Specifically, it is necessary block the certificate or remove it from the list.

If the certificate is used in multiple agreements, block or remove it from all the agreements.

3 ČSOB BUSINESS CONNECTOR INTEFACE FOR CEB FOR THIRD PARTIES

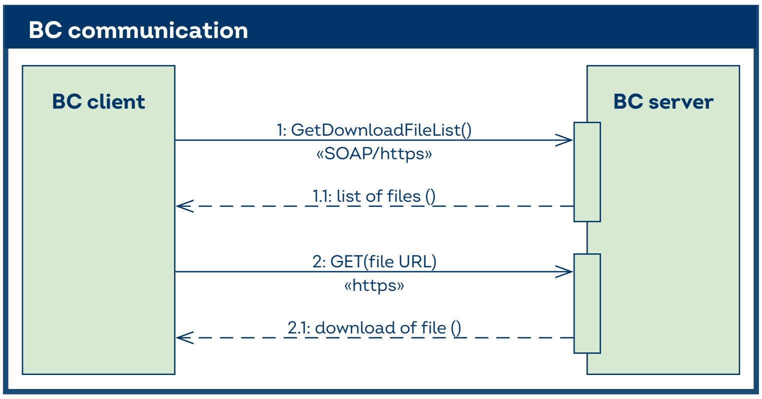
This chapter describes the technical interface of the service designed for the implementation of your own application through which you will communicate with the bank.

3.1 Principles

The ČSOB Business Connector interface is a combination of:

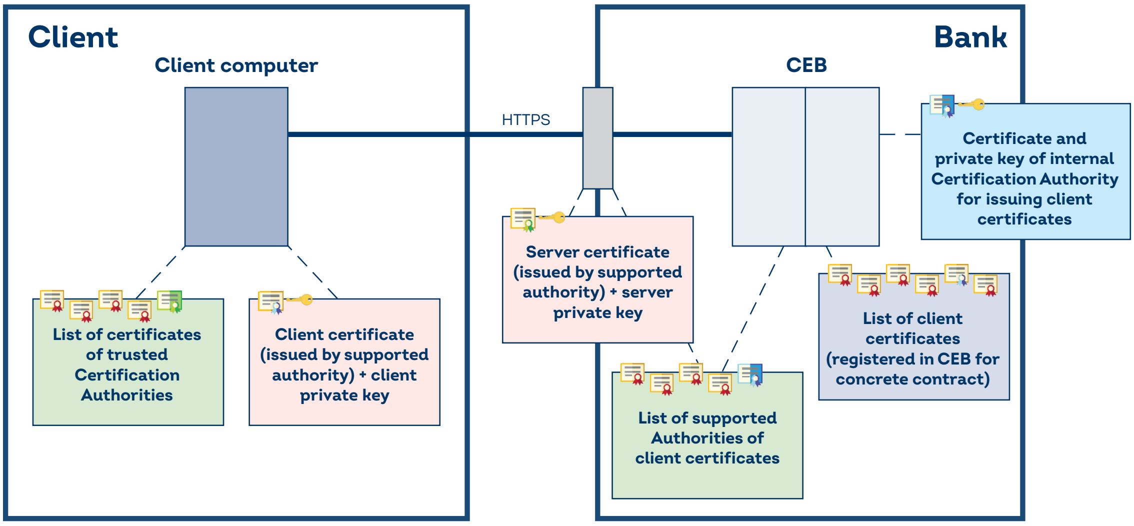
- web service using SOAP/HTTPS and
- REST service using GET and POST HTTP operations.

Web service operations coordinate and control the process, while the REST interface ensures file transfers. See the figure below:



3.1.1 Authentication

The web service (SOAP/HTTPS interface) uses an SSL connection with the mutual authentication of client and server certificates. This means that both the bank's server and the client's application verify themselves using their certificates, and the private keys belonging to the respective certificates are used for authentication. Which means that the client uses a client access SSL certificate for authentication in addition to the normal HTTPS connection. This certificate must be registered for use in the ČSOB Business Connector service; see chapter 2.2.


Client
Client computer
List of certificates of trusted Certification Authorities
Client certificate (issued by supported authority) + client private key
HTTPS
Bank
CEB
Server certificate (issued by supported authority) + server private key
Certificate and private key of internal Certification Authority for issuing client certificates
List of client certificates (registered in CEB for concrete contract)
List of supported Authorities of client certificates

📜🔑 Server certificate with private key

📜 CA Root certificate for server certificate

📜🔑 Client certificate with private key

📜 Client certificate

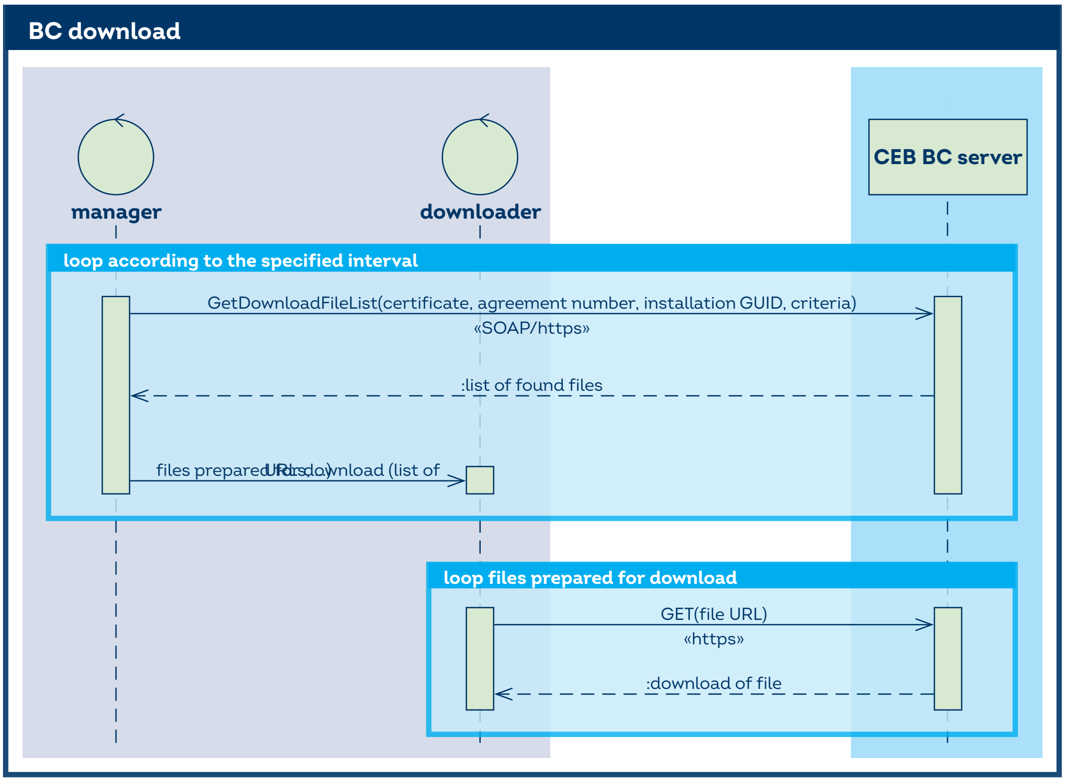
📜 CA Root certificate for client certificate

Note: The certificate of the client certificate's issuing CA should not be installed as a global trusted OS certificate. It is not usually necessary for authentication and communication. However, it may be necessary (depending on platform and implementation capabilities) to install this CA certificate e.g. in the list of trusted publishers of the client application.

The REST service (HTTPS interface) for downloading/uploading files also uses an SSL connection with the mutual authentication of client and server certificates. Additionally, the client's identity is contained in the HTTP header as well as in the URL (in an encrypted form).

3.1.2 Downloading files

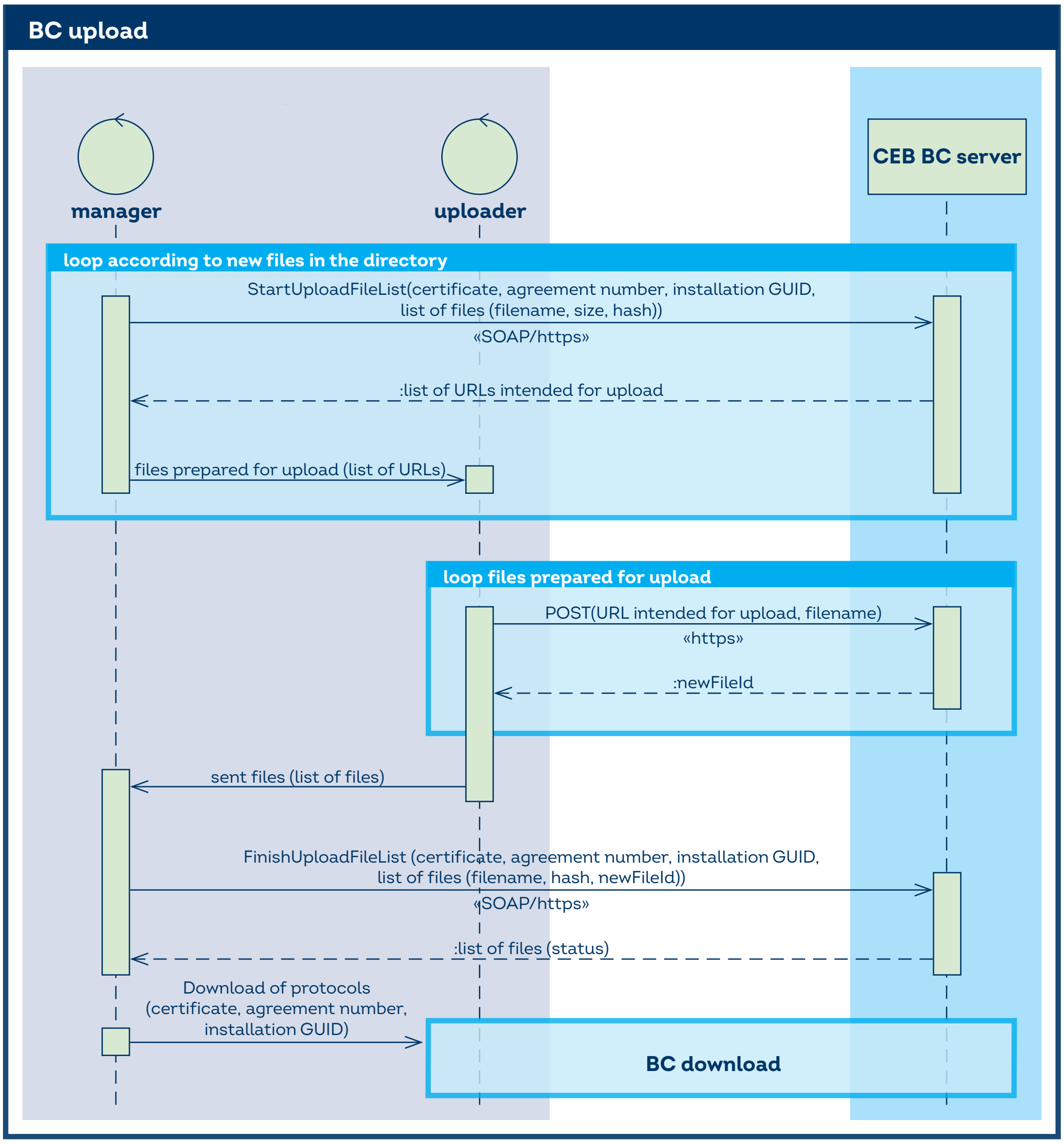
The download process should run in two threads. The manager thread regularly checks whether new files prepared for download have appeared on the server. A separate thread continuously downloads these files.


BC download
manager
downloader
CEB BC server
loop according to the specified interval
GetDownloadFileList(certificate, agreement number, installation GUID, criteria)
«SOAP/https»
:list of found files
files prepared for download (list of URLs)
loop files prepared for download
GET(file URL)
«https»
:download of file

3.1.3 Uploading files

The upload of files consists of several steps, which can be performed in separate threads. The manager thread monitors the registered directory. The thread requests the URL from the server to which the files that appear in the directory can be sent. A separate thread continuously uploads these files. After sending a file successfully (individually or in a group) the thread informs the server that the file has been sent and can be processed.

The server processes files asynchronously, generating protocols on the processing of batches, which can be downloaded as described above; see the previous chapter.


BC upload
manager
uploader
CEB BC server
loop according to new files in the directory
StartUploadFileList(certificate, agreement number, installation GUID, list of files (filename, size, hash))
«SOAP/https»
:list of URLs intended for upload
files prepared for upload (list of URLs)
loop files prepared for upload
POST(URL intended for upload, filename)
«https»
:newFileId
sent files (list of files)
FinishUploadFileList (certificate, agreement number, installation GUID, list of files (filename, hash, newFileId))
«SOAP/https»
:list of files (status)
Download of protocols (certificate, agreement number, installation GUID)
BC download

3.2 Web service (SOAP/HTTPS)

3.2.1 GetDownloadFileList operation

This method regularly checks whether new files prepared for download have been created by the bank. The client application will specify which files it monitors. The service returns a list of the files that have been found and the URLs from which the files can be downloaded via HTTP GET.

3.2.1.1 Input

Parameter	Description
ContractNumber	the number of the Agreement on the Use of the ČSOB CEB Service
PrevQueryTimestamp	[optional] the date and time from which the client is interested in new files; see chapter Monitoring new files; a time entry older than 45 days is ignored; if the parameter is not specified, the time will be set to 45 days before the current date and time; see below for format
Filter	[optional] the filter that limits the list of returned files according the specified criteria; see chapter Filtering criteria
Filter/FileTypes **Filter/FileTypes/FileType**	[optional, multiplicative] only files of the following types: VYPIS – account statements AVIZO – payment advices KURZY – CNB and ČSOB exchange rates IMPPROT – protocols on import

Filter/FileFormats **Filter/FileFormats/FileFormat**	[optional, multiplicative] only files of the following formats: – human-readable account statements: PDF, TXT, – data statements: XML, BBGPC, BBMT940, BBTXT, BBBBF, SEPAXML, – advices: MT942, BBF, CAMT052 – exchange rates: N/A, i.e. FileFormat is ignored
Filter/FileName	[optional] only the file of the specified name including the extension
Filter/CreatedAfter	[optional] only the files created after (or on) the specified date and time; see below for format
Filter/CreatedBefore	[optional] only the files created before (or on) the specified date and time; see below for format
Filter/ClientAppGuid [for uploading files]	[optional] plus the files created specifically for a given instance of the client application (e.g. import protocols)

3.2.1.1.1 Filtering criteria

The service allows you to use a list of the conditions that serve as filtering criteria, limiting the number of returned files.

The list can be limited (a combination of criteria is also possible):

- by the creation date of the file – the client can enter a from-to parameter (the **CreatedAfter** and/or **CreatedBefore** filters);
- by type – the client can select one file type, multiple types, or all types (the **FileType** filter);
- by format – the client can select a specific file format, a list of formats, or no format limits (the **FileFormat** filter);
- by name – a specific file can be downloaded (the **FileName** filter);
- not downloaded yet (the **PrevQueryTimestamp** parameter).

All time entries are in the standard xsd:dateTime format YYYY-MM-DDTHH:MM:SS+ZZ:ZZ, which means:

- **YYYY-MM-DD** – year, month, day expressed by 4 (or 2) digits; months are calculated from the 1st;
- **T** – The capital T character separates the date and time;
- **HH:MM:SS** – hour, minute and second in a 24-hour time format;
- **+ZZ:ZZ** – time zone in the numerical format HH:MM, i.e. time compared to GMT; +01:00 for Central European time and +02:00 for Central European Summer Time.

3.2.1.2 Output

Parameter	Description
QueryTimestamp	the date and time of the service call generated by the server, intended for use in the next call as the content of the PrevQueryTimestamp parameter
FileList/FileDetail	[optional, multiplicative] the list of found files
FileList/FileDetail/Url	[optional] the URL from which the file can be downloaded; if the file is currently being prepared for download or the preparation has failed, this element won't be filled in; the URL can be retrieved by a repeated query (with the original PrevQueryTimestamp)
FileList/FileDetail/Filename	the file name including the extension
FileList/FileDetail/Type	the possible types are: VYPIS – account statements AVIZO – payment advices KURZY – CNB and ČSOB exchange rates IMPPROT – protocols on import
FileList/FileDetail/Format [from version of service v3]	file format; the possible formats are: – For human-readable account statements: PDF, TXT – data statements: XML, BBGPC, BBMT940, BBTXT, BBBBF, SEPAXML – for advices: MT942, BBF, CAMT052 – for exchange rates: will not be specified
FileList/FileDetail/CreationDateTime	the date and time when the file was generated
FileList/FileDetail/Size	file size in bytes
FileList/FileDetail/UploadFileHash	[optional] for import protocols only; the sum identifying the sent file that contains payment orders for which this protocol file has been created. SHA256, MD5 up to v3. (for older protocols is MD5 padded with spaces)

FileList/FileDetail/Status	the status of the file that is being prepared for download: R – try again, the file is being prepared D – you can start the download according to the URL F – permanent error, write to log
TicketId	the unique identification of the original request to track an error in the bank

3.2.1.3 Errors

In the case of an application error, the service returns SOAP Fault, which indicates the problem that has occurred.

Parameter	Description
Code	error code, see below
Text	error message
TicketId	the unique identification of the original request to track an error in the bank

Below is the list of error codes:

Code	Description
1000	general server error
1002	the access via Business Connector is not allowed for this agreement
1011	the certificate is registered for use in the Business Connector, the agreement does not exist or is not active
1012	the certificate is blocked for use in Business Connector
1101	the access is temporarily blocked due to the excessive number of calls

3.2.1.4 Versions

Version	Description
v1	Original version – cannot be used
v2	Added TicketId to output – obsolete, usabel only if no upload is performer
v3	Added filtering by FileFormat (PDF, TXT, …) – obsolete, usable only if no upload is performed
V4	Change the format of the field UploadFileHash from MD5 to SHA256

3.2.1.5 Monitoring new files

If the *PrevQueryTimestamp* parameter is used, the service will return only the files that started to be available for download after the specified time. Your application can use this feature to monitor whether new files are available for download. The application will place the *QueryTimestamp* value, which the *GetDownloadFileList()* service returns in each response, into the *PrevQueryTimestamp* input parameter on the next call. For results to be consistent, the application must keep other parameters, such as *ContractNumber* and *Filter*, between these calls. If the service returns an error, the application must repeat the call with the original *PrevQueryTimestamp*.

If a file has already been generated in the bank, the service knows about it and returns it in the response, but it is not yet prepared for download, this will be indicated by an 'R' status of the file and the URL for download will (as yet) be missing. The client application must retry the call later with the original *PrevQueryTimestamp* until the service stops returning the list that contains a file without a URL for download. The files that are already available for download (i.e. in whose case the service returned the 'D' status and a URL) may be downloaded in the meantime. The application should use another (shorter) interval for such a recurring service call, but the minimum protection interval between calls must be observed nevertheless.

Note: The service will return only the files that were created during the period when the download of files was enabled for a given account in the Business Connector settings. The service will not return the files that had been generated by the bank before the download was enabled or were generated during the period when the download of files was temporarily disabled.

3.2.2 StartUploadFileList operation

This method is used to start the process of uploading files to the bank. The client calls this method when they want to send a file, e.g. when they find out that new files appeared in the directory. The client application sends a list containing information about the files it intends to send. The service returns a list of the URLs to which the files can be uploaded via HTTP POST.

3.2.2.1 Input

Parameter	Description
ContractNumber	the number of the Agreement on the Use of the ČSOB CEB Service
ClientAppGuid	GUID of the specific installation of the client application that made the call – a hex string in the following format is expected: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx (i.e. 8zn-4zn-4zn-4zn-12zn without without curly braces), see https://en.wikipedia.org/wiki/Universally_unique_identifier
FileList	[required, multiplicative] the list of the files the client wants to send
FileList/ImportFileDetail	file detail
FileList/ImportFileDetail/Filename	the file name including the extension; limited to 50 characters
FileList/ImportFileDetail/Hash	SHA256 sum (up to version v2 MD5 sum) file content, in case of signed files (Mode=SignedAllOrNothing) it is possible to use either the hash of the original file without signature or the hash of the whole file including all signatures (64 hex characters, up to version v3 32 characters
FileList/ImportFileDetail/Size	file size in bytes
FileList/ImportFileDetail/Format	file format (ABO, DUZ, MC TPS, MC ZPS, TXT TPS, TXT ZPS, XLS TPS, XLS ZPS, XLSX TPS, XLSX ZPS, MT101, XML SEPA, XML TPS, XML ZPS)
FileList/ImportFileDetail/Separator	[optional] field separator; characters |, /, :, ::, ; or ;; if no separator is used, it is a fixed-width file
FileList/ImportFileDetail/Mode	how to respond to import errors: IncludeIncorrect – accept also incorrect items OnlyCorrect – accept only error-free items AllOrNothing – do not accept any item if an error occurs SignedAllOrNothing [upload of signed files] – automatically authorize, but do not accept any item if an error occurs
FileList/ImportFileDetail/ SkipCheckDuplicates	[optional] true/false, default false, if it is set to true, it will not check for the same file content in the last 30 days and such a file can be sent to the bank. For Mode=SignedAllOrNothing, the duplicate check cannot be disabled and this flag will be ignored

3.2.2.2 Output

Parameter	Description
FileList	[required, multiplicative] the list of found files
FileList/FileUrl	upload detail
FileList/FileUrl/Filename	the input file name including the extension
FileList/FileUrl/Hash	the input MD5 sum of the file content (32 hex characters)
FileList/FileUrl/Status	file status: R – rejected (already imported, ...) – write to log U – you can start the download according to the URL
FileList/FileUrl/Url	[optional] the URL to which the file can be uploaded if Status = "U"
TicketId	the unique identification of the original request to track an error in the bank

3.2.2.3 Errors

In the case of an application error, the service returns SOAP Fault, which indicates the problem that has occurred.

Parameter	Description
Code	error code, see below
Text	error message
TicketId	the unique identification of the original request to track an error in the bank

Below is the list of error codes:

Code	Description
1000	general server error
1002	the access via Business Connector is not allowed for this agreement

1011	the certificate is not registered for use in Business Connector, the agreement does not exist or is not active
1012	the certificate is blocked for use in Business Connector
1101	the access is temporarily blocked due to the excessive number of calls

3.2.2.4 Versions

Version	Description
v1	URL service returns are meant for upload „octet-stream“ (see Chap. 3.3.2) – deprecated
v2	URL, service returns are meant for upload „multipart“ (see Chap. 3.3.2) – deprecated
v3	Replacement of MD5 algorithm with SHA256, option to disable checking for file duplication

3.2.3 FinishUploadFileList operation

This method is used to finish the process of uploading files to the bank. The client calls this method when they have successfully uploaded their files to the URL provided by the *StartUploadFileList()* service and want to start the processing of these files. The client application sends a list of files and their identification referring to the previous call of the *StartUploadFileList()* method and HTTP POST. The service starts asynchronous file processing. The result of the processing is later available in the form of a protocol that the client application downloads using the *GetDownloadFileList()* call.

3.2.3.1 Input

Parameter	Description
ContractNumber	the number of the Agreement on the Use of the ČSOB CEB Service
ClientAppGuid	GUID of the specific installation of the client application that made the call – a hex string in the following format is expected: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx (i.e. 8zn-4zn-4zn-4zn-12zn without curly braces), see https://en.wikipedia.org/wiki/Universally_unique_identifier
FileList	[required, multiplicative] the list of the files the client has sent
FileList/FileId	file identification
FileList/FileId/Filename	the file name including the extension; limited to 50 characters
FileList/FileId/Hash	SHA256 sum of the file content, up to v2 MD5 sum (64 hex characters, up to v2 32 hex characters)
FileList/FileId/NewFileId	encrypted ID returned by HTTP POST

3.2.3.2 Output

Parameter	Description
FileList	[required, multiplicative] the list of found files
FileList/FileStatus	upload detail
FileList/FileStatus/Filename	the input file name including the extension
FileList/FileStatus/Hash	the input SHA256 sum of the file content, up to v2 MD5 dum (64 hex characters, up to v2 32 hex characters)
FileList/FileStatus/Status	file status: R – rejected (already imported, …) → write to log, do not repeat the upload I – the import has started → schedule the download of an import protocol
TicketId	the unique identification of the original request to track an error in the bank

3.2.3.3 Errors

In the case of an application error, the service returns SOAP Fault, which indicates the problem that has occurred.

Parameter	Description
Code	error code, see below
Text	error message
TicketId	the unique identification of the original request to track an error in the bank

Below is the list of error codes:

Code	Description
1000	general server error
1002	the access via Business Connector is not allowed for this agreement
1011	the certificate is not registered for use in Business Connector, the agreement does not exist or is not active
1012	the certificate is blocked for use in Business Connector
1101	the access is temporarily blocked because the previous access occurred too recently

3.2.3.4 Versions

Version	Description
v1	Original version using MD5 hash algorithm
v2	Replacement of the MD5 hash algorithm by the SHA256 algorithm

3.2.4 WSDL and the service address

https://www.csob.cz/portal/documents/10710/15100026/cebbc-wsdl.zip

The service can be found at the following URL.

Production environment:

https://ceb-bc.csob.cz/cebbc/api

Demo environment (sandbox) for API testing:

https://testceb-bc.csob.cz/cebbc/api

3.2.5 Protection interval

The ČSOB Business Connector web service will not allow calls more frequently than is defined for a specified period of time. The number of calls is tracked for a given pair agreement number / client access certificate, and its purpose is to protect the service from overloading.

This number is currently set to 30 calls in 20 minutes (it can be changed by the bank).

The client's implementation must ensure such a mode and timing of the use of services that a 1101 error (access is blocked due to the excessive number of calls) does not occur regularly. This error can occur only if, e.g., the service is called manually outside the regular interval.

If the application executed such an amount of calls constantly, they would never be resolved due to the incessant refreshing of the timer.

If multiple client applications are running that work with the same agreement and use the same client access certificate, and provided that the download or upload interval is too short, there is a risk of the overlapping of calls between the applications, which will lead to the regular occurrence of a 1101 error. Therefore, we recommend to use a different certificate for each installation of the client application.

3.2.6 Service shutdown

In the event of a temporary shutdown, the service will return the following HTTP status:

```
503 Service Unavailable
```

3.3 REST service (HTTP download/upload)

The service is available at:

- https://ceb-bc.csob.cz/ExtFileHubDown/... for file download,
- https://ceb-bc.csob.cz/ExtFileHubUp/... for file upload as multipart.

Test environment use URL:

- https://testceb-bc.csob.cz/ceb-mock/download?id=... for downloading files and
- https://testceb-bc.csob.cz/ceb-mock/upload?id=... for uploading files.

Client application use always URL which is sent by a relevant web service GetDownloadFileList or StartUploadFileList.

3.3.1 HTTP GET (file download)

An example of a request to download a file from URL (gained from the response from the web service GetDownloadFileList).

https://ceb-bc.csob.cz/ExtFileHubDown/v2/download?id=aQGdgoeBcZdgxGco+pVDseLnBeN.

```
GET ExtFileHubDown/v2/download?id=aQGdgoeBcZdgxGco+pVDseLnBen HTTP/1.1
```

3.3.1.1 HTTP Status

The service returns the following error status codes:

HTTP Status	Content	Solution
200	OK	OK, completed
400	URL expired; files are available for download only for 15 days	NOK, end
401	authorization error	NOK, end
404	file expired; files are available for download only for 15 days	NOK, end
500	internal server error	Try again
503	service unavailable	Try again

3.3.2 HTTP POST (file upload)

3.3.2.1 File upload as multipart (only for URL from version v2 and higher of service StartUploadFileList)

An example of request to upload a file as a MIME multipart (see RFC2046 chapter 5.1):

```
POST /ExtFileHubUp/v2/upload?id=encodedValue HTTP/1.1

Content-Type: multipart/form-data; boundary=ABCDEFGH

Content-Length: <the size of the whole file>


--ABCDEFGH

Content-Disposition: form-data; name="fileupload"; filename="<file name>"

Content-Type: application/octet-stream

Content-Length: <file size>


<file content>

--ABCDEFGH--
```

HTTP header	Content
Content-Type	`multipart/form-data; boundary="<random string>"`
Content-Length	`Number of bytes of the MIME message`

See description of the http protocol for other content and presence of standard headers.

MIME part header	Content
Content-Disposition:	`attachment; filename="<file name>", where <file name> is name of the uploaded file; MIME encoding to be used particularly for CZ specific characters, see` https://tools.ietf.org/html/rfc2047
Content-Type	`application/octet-stream`
Content-Length	`File size in bytes`

3.3.2.3 Response

If successful, the service returns a JSON object of the following form:

```
{
   "Status":"201",
   "ExtFileUrl":"",
   "NewFileId":"QqGQl_Zk5e9RGphGoKv4YbAihKSeTadC"
}
```

HTTP Status	Content
Status	upload result (extended HTTP Status, see below)
ExtFileUrl	not used
NewFileId	identifier of the uploaded file

THE SERVICE RETURNS THE FOLLOWING STATUS CODES:

HTTP Status	Description	Solution
200	OK	OK, completed
201	OK, file created	OK, completed
400	Required parameters are missing in the request; file does not exist	NOK, end
401	authorization error	NOK, end
403	not authorized; URL expired	NOK, end
408	timeout	Try again
200 Status: 450	maximum file size exceeded	NOK, end
200 Status: 451	forbidden file extension	NOK, end
200 Status: 452	forbidden file type	NOK, end
200 Status: 453	the file did not pass an anti-virus scan	NOK, end
200 Status: 454	Unallowed form of URL or content, it can not be uploaded on address like this or use this content type	NOK, end
200 Status: 455	timeout	Try again
200 Status: 456	timeout	Try again
500	internal server error	Try again
502	gateway error	Try again
503	service unavailable	Try again
504	timeout	Try again

3.4 Connection errors

It is the responsibility of the client application's implementation to identify and log the reasons why connection has not been established at the:

- network level (e.g. connection timeout, DNS resolution, etc.),
- SSL level (e.g. invalid certificate, invalidated certificate, protocol version, etc.),
- HTTP level (e.g. service shutdown, timeout, not authorized, etc.),
- SOAP level (e.g. too frequently asked queries, unknown certificate, service not allowed in the agreement, etc.),

so that diagnostics could be performed correctly, and the cause of the problem identified.

3.4.1 Network-level errors

Problems at this level are caused by unstable Internet connection, configuration errors, service overload, etc., and are usually of a temporary nature. The client application should make a repeated attempt to establish connection before the user-specified interval for the identification of changes (or for uploading files) has elapsed, but not before the minimum protection interval has elapsed.

3.4.2 SSL errors (SSL Alerts)

The service returns standard error codes defined in the RFC of relevant protocols (see https://tools.ietf.org/html/rfc5878#section-4).

3.4.3 HTTP errors (HTTP Status)

The service returns standard HTTP error (status) codes to indicate HTTP-level issues (see https://tools.ietf.org/html/rfc2616#section-10).

3.5 Testing demo environment

A testing (sandbox) environment has been created for the testing of the implementation of client applications by third-party developers. The environment has the following properties.

- The interface of both web and REST services is identical to the production environment, the only difference being the domain part of the service URL, see 3.2.5.
- The responses of both web and REST services are static, partially generated by simple rules.
- The environment does not keep any status information between calls.
- The agreement number at the input of web services (ContractNumber element) is ignored.
- File filtering criteria for GetFileDownloadList are ignored.
- The services do not require that the protection interval be observed, see 3.2.5.
- Authentication with a certificate is required, but it does not affect the content of messages.
- Certificates issued by the same certification authorities as in the production environment, including certificates issued internally by ČSOB, as well as testing certificates of these certification authorities are accepted.
- Your certificate doesn't have to be registered in CEB, nor is it required to have a CEB.

3.6 Technical requirements

3.6.1 Client certificate parameters

A certificate and a private key used by the client must meet the following requirements:

Requirement	
certificate issuer	**I.CA:** – C=CZ, O=První certifikační autorita, a.s., CN = I.CA Root CA/RSA 05/2022, serialNumber=NTRCZ-26439395 Not Before: May 03 12:05:00 2022 GMT Not After : May 03 12:05:00 2047 GMT SHA-1:461fdd19e71cd4329aadf224dc8c8628cd10fae8 – C=CZ, O=První certifikační autorita, a.s., CN=I.CA Root CA/ECC 05/2022, serialNumber=NTRCZ-26439395 Not Before: May 03 12:10:00 2022 GMT Not After : May 03 12:10:00 2047 GMT SHA-1: 702723132527203947e0a97829a0731372b03917 – C=CZ, O=První certifikační autorita, a.s., CN = I.CA Root CA/RSA 05/2022, serialNumber=NTRCZ-26439395 Not Before: Jun 20 12:00:22 2022 GMT Not After : Jun 17 12:00:22 2032 GMT SHA-1: 000c90caa3a95065fd2e5d7836bd45eeed38c18f – C=CZ, O=První certifikační autorita, a.s., CN = I.CA Root CA/ECC 05/2022, serialNumber=NTRCZ-26439395 Not Before: Jun 20 12:52:24 2022 GMT Not After : Jun 17 12:52:24 2032 GMT SHA-1: 6aa1d638ce08e8ff85c617e6b4b4c5cb1541b999 – C=CZ, O=První certifikační autorita, a.s., CN=I.CA Root CA/RSA, serialNumber=NTRCZ-26439395 Not Before: May 27 12:20:00 2015 GMT Not After : May 27 12:20:00 2040 GMT SHA-1: 9b0959898154081bf6a90e9b9e58a4690c9ba104 – C=CZ, CN=I.CA Public CA/RSA 07/2015, O=První certifikační autorita, a.s., serialNumber=NTRCZ-26439395 Not Before: Jul 8 12:36:40 2015 GMT Not After : Jul 5 12:36:40 2025 GMT SHA-1: a9d6b0afdd51691a2f9130d9af998c8195f97a83

	– C=CZ, CN=I.CA SSL CA/RSA 07/2015, O=První certifikační autorita, a.s., serialNumber=NTRCZ-26439395 Not Before: Jul 8 12:18:18 2015 GMT Not After : Jul 5 12:18:18 2025 GMT SHA-1: 984fd6ba71dbb50fe2aca83e476d4f61584d4243 **PostSignum:** – C=CZ, O=Česká pošta, s.p. [IČ 47114983], CN=PostSignum Root QCA 2 Not Before: Jan 19 09:04:31 2010 GMT Not After : Jan 19 09:04:31 2025 GMT SHA-1: A0F8DB3F0BF417693B282EB74A6AD86DF9D448A3 – C=CZ, O=Česká pošta, s.p. [IČ 47114983], CN=PostSignum Public CA 3 Not Before: Mar 20 09:28:38 2017 GMT Not After : Jan 19 09:04:31 2025 GMT SHA-1: 92A04A6805AD4317234F11D16B583981A64F02A1 – C=CZ, O=Česká pošta, s.p., CN=PostSignum Root QCA 4 Not Before: Jul 26 09:56:08 2018 GMT Not After : Jul 26 09:56:08 2038 GMT SHA-1: aa40d2579ba82424cd27719b1d6b1f3571738099 – C=CZ, O=Česká pošta, s.p., CN=PostSignum Public CA 4, 2.5.4.97=NTRCZ-47114983 Not Before: Sep 27 10:19:35 2018 GMT Not After : Sep 27 10:19:35 2033 GMT SHA-1: 1311e16d9903f914167e222b2326f699d4835fee – C=CZ, O=Česká pošta, s.p., CN=PostSignum Public CA 5, 2.5.4.97=NTRCZ-47114983 Not Before: Oct 03 06:48:01 2018 GMT Not After : Oct 03 06:48:01 2033 GMT SHA-1: a6147a88433278d9ab1e655bb8ba315fec4640d2 **Certificates issued internally by ČSOB Business Connector:** – CN= CEB Business Connector CA, O=Československá obchodní banka a.s., C=CZ, S = Prague Not Before: Mar 21 13:01:22 2018 Not After : Mar 21 13:01:22 2028 SHA-1: A72CA62B0A214EBB1904EF9B1D5574A71EDB649E
signature algorithm	SHA256 or stronger
key length	RSA at least 2048 bits
use of key (if relevant)	Digital signature or Exchange of keys
extended use of key (if relevant)	SSL client authentication

3.6.2 Requirements on SSL connection

The client application must create an SSL connection using the latest possible version of the SSL/TLS protocol.

The bank's server has the following requirements:

Requirement	
SSL/TLS version	TLS 1.3 recommended, at least TLS 1.2
certificate subject on the bank's side	CN=ceb-bc.csob.cz attribute others not specified
certificate issuer on the bank's side	standard trusted certification authority registered in Windows

3.6.3 Requirements on HTTP and SOAP

Requirement	
HTTP version	HTTP 1.1 nebo HTTP 1.0
SOAP version	SOAP 1.1

required HTTP headers	`Content-Type: text/xml; charset=utf-8`
	`SOAPAction: "{operation}"`
	where {operation} is value of atribute soapAction from WSDL element <soap:operation>
	Content-Length: {length of body of the message in bytes}

4 FILE FORMATS

4.1 Statements

For a description of the format structure of statements received from ČSOB Business Connector, please visit www.csob.cz/ceb.

4.2 Advices

For a description of the format structure of advices received from ČSOB Business Connector, please visit www.csob.cz/ceb.

4.3 Exchange rates

Format of Exchange rates received from ČSOB Business Connector – QUOTES message.

The file name is:

- EXRT_CNB_yyyymmdd.BBF for CNB Exchange rates;
- EXRT_CNB_yyyymmdd.BBF for ČSOB Exchange rates.

A QUOTES message consists of one header entry and two types of data records.

The length Header 01 is 32, and it looks as follows:

QUOTES – RECORD 01 (1 occur – first record)					
Name	**Type**	**L**	**Pos**	**M/O**	**Description**
Banking aplication	C	1	1	M	Banking application, const. T
Client identification	C	8	2	M	Client identification
Message type	C	6	10	M	Message type
Separator	C	1	16	M	Separator – 1 space
Record type	C	2	17	M	Record type:"01" – Message header
Unique message number	C	14	19	M	Unique identification of message

The records are distinguished by the "record type" (rec_typ) item in the service items at the beginning of the record:

- Record containing general data; rec_typ is "02". This record contains general QUOTES message data. The record occurs 1.
- Record containing exchange rates; rec_typ is "03". This record contains exchange rates for one currency. The record occurs 1–9999. The record is subordinate to "02".

The length of record 02 is 76, and it looks as follows:

QUOTES – RECORD 02					
Name	**Type**	**L**	**Pos**	**M/O**	**Description**
Banking application	C	1	1	M	Banking application, const. "N"
Client identification	C	8	2	M	BB identification of client's application
Message type	C	6	10	M	Type of EDIFACT message – QUOTES
Separator	C	1	16	M	Separator – 1 space
Record type	C	2	17	M	Record type: "02" – Data record
Serial number	N	3	19	O	Serial number of the Exchange rates
Start date	D	8	22	M	Exchange rates validity start date; FORMAT=„CCYYMMDD“
Source name	C	35	30	M	Source (provider) name
Timestamp	C	12	65	M	Timestamp

The length of record 03 is 124, and it looks as follows:

QUOTES – RECORD 03					
Name	**Type**	**L**	**Pos**	**M/O**	**Description**
Banking application	C	1	1	M	Banking application, const. „N“
Client identification	C	8	2	M	BB identification of client's application
Message type	C	6	10	M	Type of EDIFACT message – QUOTES
Separator	C	1	16	M	Separator – 1 space
Record type	C	2	17	M	Record type: "03" – Data record
Country	C	35	19	M	Country name
Amount	N	4	54	M	Amount
filler2	C	2	58	M	
Currency code	C	3	60	M	Currency code
filler3	C	1	63	M	
FX buy	N	10.3	64	M	FOREIGN EXCHANGE / Buy exchange rate
FX sell	N	10.3	74	M	FOREIGN EXCHANGE / Sell exchange rate
FX middle	N	10.3	84	M	FOREIGN EXCHANGE / Middle exchange rate
filler4	C	1	94	M	
FX cash buy	N	10.3	95	M	FOREIGN CURRENCY / Buy exchange rate
FX cash sell	N	10.3	105	M	FOREIGN CURRENCY / Sell exchange rate
FX cash middle	N	10.3	115	M	FOREIGN CURRENCY / Middle exchange rate

Note: The exchange rate format is "C.D" 6 places + "." + 3 places

Example of file with foreign exchange rates:

```
TTDCEB   QUOTES 0120180831057299
NTDCEB   QUOTES 0216820180831CSOB                              201808310656
NTDCEB   QUOTES 03AUSTRALIAN DOLLAR                     1  AUD     15.617    16.415    16.016     0.000     0.000     0.000
NTDCEB   QUOTES 03CANADIAN DOLLAR                       1  CAD     16.553    17.400    16.977     0.000     0.000     0.000
NTDCEB   QUOTES 03SWISS FRANC                           1  CHF     22.244    23.385    22.815    22.244    23.385    22.815
NTDCEB   QUOTES 03CHINA JUAN                            1  CNY      3.033     3.421     3.227     0.000     0.000     0.000
NTDCEB   QUOTES 03DANISH KRONER                         1  DKK      3.371     3.543     3.457     3.371     3.543     3.457
NTDCEB   QUOTES 03EUROPEAN CURRENCY UNIT                1  EUR     25.135    26.412    25.773    25.135    26.412    25.773
NTDCEB   QUOTES 03BRITISH POUND                         1  GBP     28.027    29.459    28.743    28.027    29.459    28.743
NTDCEB   QUOTES 03CHORVATSKA KUNA                       1  HRK      3.375     3.555     3.465     0.000     0.000     0.000
NTDCEB   QUOTES 03HUNGARIAN FORINT                    100  HUF      7.681     8.080     7.881     0.000     0.000     0.000
NTDCEB   QUOTES 03JAPANESE YEN                        100  JPY     19.406    20.397    19.901     0.000     0.000     0.000
NTDCEB   QUOTES 03NORWEGIAN KRONER                      1  NOK      2.581     2.714     2.647     2.581     2.714     2.647
NTDCEB   QUOTES 03POLISH ZLOTY                          1  PLN      5.840     6.144     5.992     0.000     0.000     0.000
NTDCEB   QUOTES 03RUMANIAN LEI                          1  RON      5.407     5.685     5.546     0.000     0.000     0.000
NTDCEB   QUOTES 03RUSSIAN ROUBLE                      100  RUB     30.444    34.349    32.396     0.000     0.000     0.000
NTDCEB   QUOTES 03SWEDISH KRONER                        1  SEK      2.361     2.482     2.421     2.361     2.482     2.421
NTDCEB   QUOTES 03TURECKÁ LIRA                          1  TRY      3.016     3.544     3.280     0.000     0.000     0.000
NTDCEB   QUOTES 03UNITED STATES DOLLAR                  1  USD     21.547    22.645    22.096    21.547    22.645    22.096
```

4.4 Batch payment orders

PFor a description of the format structure of the import of batch payment orders to the ČSOB CEB service, please visit www.csob.cz/ceb.

4.5 Import protocol

Format of the export file Protocol on import from the ČSOB Business Connector service:

Import protocol format	XSD pain.002 (ČSOB) and description of the protocol format
XML PAIN.002 – import protocol *- output protocol on the successful/ unsuccessful import of batch payment orders, based on the ISO20022 SWIFT pain.002 standard*	https://www.csob.cz/portal/documents/10710/15100026/protokol-pain-en.zip

4.6 Signed batch payment orders

This is the same set of file types as in the previous chapter. Additionally, an internal electronic signature in the CAdES-BES format is inserted in the file. Also, the .p7m extension has been added (which means the file contains two extensions, e.g. 125456_10000141.zps.p7m). This file is not a text file, but the text information in it is not encrypted.

The file must be signed with a certificate (on a chip card) that is intended for working on the CEB portal and authorizing transactions in the waiting room – i.e. not with a client access certificate, intended for ČSOB Business Connector, which is discussed in chapter 2!

A CAdES-BES signature must be created in accordance with the following standards:

- ETSI TS 101 733 (v2.1.1) at the BES compliance level.
- ETSI EN 319 122-1 at the B-B compliance level.
- ETSI TS 103 173 at the B compliance level.

With the following restrictive conditions:

- The following attributes are supported inside signatures: content-type, signing-time, signing-certificate (i.e. ESS signing-certificate or ESS signing-certificate v2), message-digest. Any other attributes are ignored and not checked during the verification process.
- Signatures with defined signature policy are not supported.

Multisignature support:

The verification of parallel (independent) signatures is supported. The verification of other types of multisignatures is not supported.

Neither the ČSOB Business Connector service nor the client application enable the creation of signed payment order files. However, third-party commercial software can be used due to the standard signature format.